



HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10011529-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Tom Howard et al.
Application No.: 10/037,267
Filing Date: January 2, 2002

Confirmation No.: 6181
Examiner: T.M. Szymanski
Group Art Unit: 2134

Title: SYSTEM AND METHOD FOR PREVENTING USE OF A WIRELESS DEVICE

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 2/16/2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month
\$120

☐ 2nd Month
\$450

☐ 3rd Month
\$1020

☐ 4th Month
\$1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 500 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV628782652US in an envelope addressed to: MS Appeal Brief-Patents Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: April 6, 2006

Typed Name: Donna Forbit

Signature: Donna Forbit

Respectfully submitted,

Tom Howard et al

By Michael A. Papalas

Michael A. Papalas

Attorney/Agent for Applicant(s)

Reg No. : 40,381

Date : April 6, 2006

Telephone : 214-855-8186

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400



Docket No.: 10011529-1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Tom Howard et al.

Application No.: 10/037,267

Confirmation No.: 6181

Filed: January 2, 2002

Art Unit: 2134

For: SYSTEM AND METHOD FOR PREVENTING
USE OF A WIRELESS DEVICE

Examiner: T. M. Szymanski

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on February 16, 2006, and is in furtherance of said Notice of Appeal.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

- | | |
|-------|---|
| I. | Real Party In Interest |
| II | Related Appeals and Interferences |
| III. | Status of Claims |
| IV. | Status of Amendments |
| V. | Summary of Claimed Subject Matter |
| VI. | Grounds of Rejection to be Reviewed on Appeal |
| VII. | Argument |
| VIII. | Claims |
| IX. | Evidence |
| X. | Related Proceedings |

04/10/2006 HABBELR1 00000001 082025 10037267

01 FC:1402 500.00 DA

04/10/2006 HABBELR1 00000002 082025 10037267
01 FC:1402 500.00 DA

Appendix A	Claims
Appendix B	Evidence
Appendix C	Related Proceedings

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Hewlett-Packard Development Company, L.P., a Texas Limited Partnership, having its principal place of business in Houston, Texas.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 17 claims pending in application.

B. Current Status of Claims

1. Claims canceled: 8, 10 and 20. It should be noted that Appellant canceled claim 20 in an amendment filed concurrently with this Brief.
2. Claims withdrawn from consideration but not canceled: None. Please note that page 1 of the Final Office Action indicates that claims 8, 10, and 20 are withdrawn from consideration. It is believed that such indication is in error for at least two reasons. First, no restriction requirement has been made. Second, claims 8 and 10 were canceled before the Final Office Action issued.
3. Claims pending: 1-7, 9, and 11-19
4. Claims allowed: None
5. Claims rejected: 1-7, 9, and 11-19

C. Claims On Appeal

The claims on appeal are claims 1-7, 9, and 11-19.

IV. STATUS OF AMENDMENTS

Appellant did not file an Amendment After Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

According to claim 1, a processor-based device that prevents unauthorized use comprises a processor for executing software instructions (102 of figure 1); software instructions defining at least one user application (107 of figure 1 and paragraph [0021]); a wireless communication subsystem that is operable to transmit and receive data utilizing a wireless protocol (101 of figure 1 and paragraph [0015]); software instructions defining a security protocol process that is operable to prevent execution of said software instructions defining said at least one user application by said processor when a message is received via said wireless communication subsystem, wherein said message indicates that said processor-based device is not in possession of a rightful user (110 of figure 1, 500 of figure 5, and paragraphs [0029]-[0032]); and a basic input/output system (BIOS) that is operable to boot said processor-based device and is further operable to verify integrity of said security protocol process before completing boot operations (105 of figure 1 and paragraph [0020]).

According to claim 2, the system of claim 1 further comprises non-volatile memory, wherein said security protocol process is operable to store information in said non-volatile memory to indicate that execution of said software instructions defining at least one user application is not permitted (106 of figure 1, 503 of figure 5, and paragraph [0030]).

According to claim 6, the system of claim 1 further comprises a display, wherein said security protocol process causes said display to present information indicating that said rightful user is not in possession of said processor-based device (109 of figure 1, 506 of figure 5, and paragraph [0031]).

According to claim 7, the system of claim 1 further comprises a feature wherein said security protocol process is implemented in an operating system of the processor-based device (103 of figure 1 and paragraphs [0017]-[0019]).

According to claim 9, a method for protecting a processor-based device from unauthorized use, wherein the processor-based device performs wireless communication, the method comprising: receiving notice that said processor-based device is not in possession of a rightful user (201 of figure 2 and paragraph [0022]); sending a message to said processor-based device to initiate a security protocol via a wireless communication protocol (203 of figure 2 and paragraph [0024]); receiving said message by said processor-based device (501 of figure 5 and paragraph [0029]); and initiating said security protocol on said processor-based device in response to said received message, wherein said initiating comprises preventing execution by said processor-based device of at least one user application that is defined by software instructions stored on said processor-based device in response to receiving said message by said processor-based device (503-505 of figure 5 and paragraphs [0030]-[0031]); and writing information in non-volatile memory of said processor-based device that said processor-based device is not in possession of said rightful user in response to said received message (503 of figure 5 and paragraph [0030]).

According to claim 13, the method of claim 9 further comprises displaying a message on a display of said processor-based device to indicate that said processor-based device is not in possession of said rightful user (506 of figure 5 and paragraph [0031]).

According to claim 16, a system that prevents unauthorized use comprises means for processing software instructions (e.g., 102 of figure 1); means for defining at least one user application (e.g., paragraph [0021]); means for transmitting and receiving data utilizing a wireless communication protocol (e.g., 101 of figure 1 and paragraph [0015]); and means for preventing execution of said software instructions defining said at least one user application by said means for processing when a message is received via said means for transmitting and receiving (e.g., 110 of figure 1 and paragraphs [0029]-[0032]), wherein said message indicates that said system is not in possession of a rightful user (paragraph [0024]), wherein said means for preventing execution is implemented by an operating system of said system (103 of figure 1 and paragraphs [0017]-[0019]).

According to claim 19, the system of claim 16 further comprises means for displaying information to indicate that said rightful user is not in possession of said system (e.g., 109 of figure 1, 506 of figure 5, and paragraph [0031]).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-7, 9, and 11-19 are rejected under 35 U.S.C. §103(a) as being obvious over US 5,987,609 (hereinafter, *Hasebe*), in view of US Publication 2002/0004905 (hereinafter, *Davis*) in further view of US Publication 2001/0045884 (hereinafter, *Barrus*). This is the sole ground of rejection.

VII. ARGUMENT

Claims 1-7, 9, and 11-19 are rejected under 35 U.S.C. §103(a) as being obvious over *Hasebe* in view of *Davis* in further view of *Barrus*. Appellant traverses the rejection.

A. Claims 1 and 3-5

To show obviousness under 35 U.S.C. § 103(a), three basic criteria must be met. First, there must be some suggestion or motivation, either in the reference itself or in the knowledge generally available to one of ordinary skill in the art, to modify the applied reference. See *In re Vaeck* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Second, there must be a reasonable expectation of success. *In re Merck and Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Finally, the applied reference must teach or suggest all the claim

limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Without conceding any other criteria, Appellant respectfully asserts that the rejection does not satisfy the third criterion, as discussed further below.

Claim 1 recites, in part, “a basic input/output system (BIOS) that is operable to boot said processor-based device and is further operable to verify integrity of said security protocol process before completing boot operations.” The Office Action does not rely upon *Hasebe* or *Barrus* to teach or suggest this feature, nor do *Hasebe* or *Barrus* teach or suggest this feature. Further, *Davis* does not teach or suggest this feature, contrary to the Examiner’s assertion, because *Davis* does not teach or suggest a BIOS that is operable to verify integrity of a security protocol. Paragraph [0018] of *Davis*, cited by the Office Action, does not teach or suggest a BIOS that verifies integrity of a security protocol. In fact, *Davis* teaches a system that authenticates BIOS code, rather than a BIOS that verifies integrity of a security protocol. *See Davis* at Abstract. Accordingly, the combination of *Hasebe*, *Davis*, and *Barrus* does not teach or suggest at least the above-quoted feature of claim 1.

In the Response to Arguments section of the Final Action, the Examiner states:

In the case of this combination the BIOS itself is inclusive to a security protocol as the software is responsible for access and loading of the system (*Davis* Paragraphs 4-10) and as stated contains built in security methods lending itself to be understood as a security protocol by the broadest reasonable interpretation of the Appellant’s claim.

Final Action at 6. Thus, it appears that the Examiner is asserting either that the BIOS of *Davis* includes a security protocol or that the BIOS and a security protocol are one in the same. However, either interpretation is incorrect. *Davis* teaches that the software code to authenticate the BIOS is separate from the BIOS. Note that IC device 520 of figure 5 of *Davis* includes software code to authenticate the BIOS. *See Davis* at Abstract, paragraph [0030] and figure 5. IC device 520 is part of cryptographic device 410 of figure 4. The cryptographic device 410 is separate from the BIOS device (1701 of figure 1), as described in paragraph [0037]—“[t]he host processor temporarily acts as a Direct Memory Access (DMA) device between the BIOS device and the cryptographic device.” Thus, the two are separate, and one does not include the other.

The Examiner's assertion is further contradicted by the Abstract of *Davis* that states, "the second IC device includes logic circuitry to execute a software code to authenticate the BIOS code before permitting execution of the BIOS code by the host processor." Thus, the software code must be executed before the BIOS can be executed, and the two cannot be the same. Accordingly, neither Hasebe, Davis, nor Barrus teach or suggest the above-recited feature of claim 1.

Dependent claims 3-5 each depend either directly or indirectly from independent claim 1 and, thus, inherit all of the limitations of independent claim 1. Thus, the cited combination does not teach or suggest all claim limitations of claims 3-5. It is respectfully submitted that dependent claims 3-5 are allowable at least because of their dependence from claim 1 for the reasons discussed above. Thus, Appellant respectfully requests that the 35 U.S.C. §103(a) rejection of claims 1 and 3-5 be reversed.

B. Claim 2

Claim 2 is allowable at least because of its dependence from claim 1. Additionally, claim 2 recites features that are novel and non-obvious in their own right. For instance, claim 2 recites in part, "non-volatile memory, wherein said security protocol process is operable to store information in said non-volatile memory to indicate that execution of said software instructions defining at least one user application is not permitted." The rejection does not rely on *Davis* or *Barrus* to teach or suggest the feature, nor do *Davis* or *Barrus* teach or suggest the feature. Instead, the rejection relies on *Hasebe* at the passage at column 4, line 45 through column 6, line 65. Final Action at 4. However, as noted below with regard to independent claim 9, *Hasebe* teaches using random-access memory (RAM) to store everything other than programs, for example, password information and security level information. See *Hasebe* at Col. 4, lines 49-65, Col. 6, lines 56-58, and figure 3. Thus, since RAM is volatile, rather than non-volatile, *Hasebe* does not teach or suggest the above-recited feature of claim 2. Since the cited combination does not teach or suggest this feature of claim 2, reversal of the 35 U.S.C. § 103(a) rejection of claim 2 is respectfully requested.

C. Claim 6

Claim 6 is allowable at least because of its dependence from claim 1. Additionally, claim 6 recites features that are novel and non-obvious in their own right. For instance, claim

6 recites in part, “a display, wherein said security protocol process causes said display to present information indicating that said rightful user is not in possession of said processor-based device.” The rejection does not rely on *Davis* or *Barrus* to teach or suggest the feature, nor do *Davis* or *Barrus* teach or suggest the feature. Instead, the rejection relies on *Hasebe* at the passage at column 6, lines 49-55 and item 17 of figure 3. Final Action at 5. The cited passage from *Hasebe* teaches a “screen lock” function; however, a screen lock function does not teach or suggest the above recited feature because it does not cause the “display to present information indicating that said rightful user is not in possession.” In other words, locking the screen is not enough, without more, to teach or suggest causing the “display to present information indicating that said rightful user is not in possession of said processor-based device,” as recited by claim 6. Since the cited combination does not teach or suggest this feature of claim 6, reversal of the 35 U.S.C. § 103(a) rejection of claim 6 is respectfully requested.

D. Claim 7

Claim 7 is allowable at least because of its dependence from claim 1. Additionally, claim 7 recites features that are novel and non-obvious in their own right. For instance, claim 7 recites in part, “said security protocol process is implemented in an operating system of the processor-based device.” The rejection does not rely on *Davis* or *Barrus* to teach or suggest the feature, nor do *Davis* or *Barrus* teach or suggest the feature. Instead, the rejection relies on *Hasebe* at the passage at column 5, line 55-67 through column 6, line 67 and figure 3. Final Action at 5. However, as noted below with regard to independent claim 16, *Hasebe* merely teaches that a security program is stored in Read Only Memory (ROM). *Hasebe* at Col. 6, lines 60-67. Storage in ROM is not enough, by itself, to teach “implemented by an operating system” because *Hasebe* does not mention or teach that the security program (or any other module in the cited ROM) is implemented by an operating system. Further, an application that runs on top of an operating system does not teach or suggest, a “security protocol process is implemented in an operating system.” Since the cited combination does not teach or suggest this feature of claim 7, reversal of the 35 U.S.C. § 103(a) rejection of claim 7 is respectfully requested.

E. Claims 9, 11, 12, 14, and 15

Claim 9 recites, in part, “writing information in non-volatile memory of said processor-based device that said processor-based device is not in possession of said rightful user in response to said received message.” The combination of *Hasebe*, *Davis*, and *Barrus* does not teach or suggest at least this feature of claim 9. The Examiner does not rely on *Barrus* to teach or suggest the feature, nor does *Barrus* teach or suggest the feature. However, it is unclear from the rejection which portions of *Hasebe* and *Davis* are relied upon to teach or suggest this feature; thus Appellant addresses both *Hasebe* and *Davis* in detail.

First, *Hasebe* does not teach at least this feature of claim 9. *Hasebe* teaches using random-access memory (RAM) to store everything other than programs, for example, password information and security level information. See *Hasebe* at Col. 4, lines 49-65, Col. 6, lines 56-58, and figure 3. Thus, since RAM is volatile, rather than non-volatile, *Hasebe* does not teach or suggest the above-recited feature of claim 9. In Response to Arguments, the Examiner notes, “*Hasebe* references the necessary security level, contained in RAM, and the processors comparison of that to the provided information, (Col 4 line 45 – Col 6 line 65).” However, this does not rebut Appellant’s argument at all. Accordingly, *Hasebe* does not teach or suggest the above-recited feature of claim 9. The Examiner further continues, “When in combination with the reference of *Davis* et al this clearly teaches the use of non-volatile memory to store information relating to the access of the system.” However, as shown below, *Davis* also fails to teach or suggest the feature.

It is unclear which portion of *Davis* the Examiner may be relying upon. However, it should be noted that *Davis* teaches a system that authenticates the BIOS code prior to BIOS execution. See *Davis* at Abstract. *Davis* does not mention or teach that a device may not be in the possession of a rightful user, and thus, does not teach or suggest the above-recited feature of claim 9. Accordingly *Davis* does not teach or suggest the above-recited feature of claim 9.

Thus, neither *Hasebe*, *Davis*, nor *Barrus* teaches or suggests “writing information in non-volatile memory of said processor-based device that said processor-based device is not in possession of said rightful user in response to said received message,” as recited by claim 9.

Dependent claims 11, 12, 14, and 15 each depend either directly or indirectly from independent claim 9 and, thus, inherit all of the limitations of independent claim 9. Thus, the cited combination does not teach or suggest all claim limitations of claims 11, 12, 14, and 15. It is respectfully submitted that dependent claims 11, 12, 14, and 15 are allowable at least because of their dependence from claim 9 for the reasons discussed above. Accordingly, Appellant respectfully requests that the 35 U.S.C. §103(a) rejection of claims 9, 11, 12, 14, and 15 be reversed.

F. Claim 13

Claim 13 is allowable at least because of its dependence from claim 9. Additionally, claim 13 recites features that are novel and non-obvious in their own right. For instance, claim 13 recites in part, “displaying a message on a display of said processor-based device to indicate that said processor-based device is not in possession of said rightful user.” As explained above with regard to claim 6, the cited passage from *Hasebe* teaches a “screen lock” function; however, a screen lock function does not teach or suggest the above recited feature because it does not display “a message on a display ... to indicate that said processor-based device is not in possession of said rightful user.” In other words, locking the screen is not enough, without more, to teach or suggest displaying “a message ... to indicate that said processor-based device is not in possession of said rightful user,” as recited by claim 13. It appears that the rejection does not rely on *Davis* or *Barrus* to teach or suggest the feature, nor do *Davis* or *Barrus* teach or suggest the feature. Since the cited combination does not teach or suggest this feature of claim 13, reversal of the 35 U.S.C. § 103(a) rejection of claim 13 is respectfully requested.

G. Claims 16-18

Claim 16 recites, in part, “wherein said means for preventing execution is implemented by an operating system of said system.” The combination of *Hasebe*, *Davis*, and *Barrus* does not teach or suggest this feature of claim 16. The rejection does not rely on *Davis* or *Barrus* to teach or suggest the feature, nor do *Davis* or *Barrus* teach or suggest the feature. It appears the Examiner relies on the reasoning in the rejection of claim 7 to address this feature of claim 16. *See* Final Action at 5, paragraphs 17 and 18. However, *Hasebe* does not teach or suggest this feature of claim 16. The rejection cites *Hasebe* at figure 3, item 12,

column 5, lines 56-67, and column 6, lines 1-67, as teaching the feature. *Id.* at 5. The Examiner further alleges that “the security protocol must be implemented within the operating system as it is part of the system and wouldn’t have functionality independently,” and that “the system software is contained together as separate modules reliant upon the operating system.” *Id.* The statements from the Final Action are incorrect, as discussed below.

First, figure 3 of *Hasebe* merely teaches that a security program is stored in Read Only Memory (ROM). *Hasebe* at Col. 6, lines 60-67. Storage in ROM is not enough, by itself, to teach “implemented by an operating system” because *Hasebe* does not mention or teach that the security program (or any other module in the cited ROM) is implemented by an operating system.

Second, the Examiner’s statement that the security program of *Hasebe* must be implemented within an operating system is incorrect, as other configurations are possible—e.g., applications are commonly implemented to run on top of the operating system. Thus, not only does *Hasebe* not teach “implemented by an operating system,” but other configurations are possible. An application that provides security functionality and runs on top of an operating system and/or is reliant upon such operating system is different than implementing such functionality “by the operating system” itself. No teaching (either express or inherent) is provided in *Hasebe* that its software is “implemented by” an operating system of the system that is being protected, as recited by claim 16.

In response, the Examiner asserts that the claim language “implemented by an operating system” is not distinguishable from running on top of an operating system. However, the Examiner fails to give proper weight to the claim language. Clearly, “implemented by an operating system,” is not taught or suggested by an application that “runs on top of” an operating system. Accordingly, neither *Hasebe*, *Davis*, nor *Barrus* teach or suggest this feature of claim 16.

Dependent claims 17 and 18 each depend either directly or indirectly from independent claim 16 and, thus, inherit all of the limitations of independent claim 16. Thus, the cited combination does not teach or suggest all claim limitations of claims 17 and 18. It is respectfully submitted that dependent claims 17 and 18 are allowable at least because of

their dependence from claim 16 for the reasons discussed above. Accordingly, the 35 U.S.C. §103(a) rejection of claims 16-18 should be reversed.

H. Claim 19

Claim 19 is allowable at least because of its dependence from claim 16. Additionally, claim 19 recites features that are novel and non-obvious in their own right. For instance, claim 19 recites in part, “means for displaying information to indicate that said rightful user is not in possession of said system.” As explained above with regard to claim 6, the cited passage from *Hasebe* teaches a “screen lock” function; however, a screen lock function does not teach or suggest the above recited feature because it does not perform the function, “displaying information to indicate that said rightful user is not in possession of said system.” In other words, locking the screen is not enough, without more, to teach or suggest “displaying information to indicate that said rightful user is not in possession of said system,” as recited by claim 19. It appears that the rejection does not rely on *Davis* or *Barrus* to teach or suggest the feature, nor do *Davis* or *Barrus* teach or suggest the feature. Since the cited combination does not teach or suggest this feature of claim 19, reversal of the 35 U.S.C. § 103(a) rejection of claim 19 is respectfully requested.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A. As indicated above, the claims in Appendix A include the amendments filed by Appellant on November 10, 2005 in response to the non-final Office Action.

IX. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted in Appendix B.

X. RELATED PROCEEDINGS

No related proceedings are referenced in II above; thus, there are no copies of decisions in related proceedings provided in Appendix C.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV628782652US in an envelope addressed to: MS Appeal Brief-Patents Commissioner for Patents, Alexandria, VA 22313.

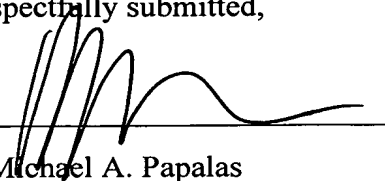
Date of Deposit: April 6, 2006

Typed Name: Donna Forbit

Signature: Donna Forbit

Respectfully submitted,

By


Michael A. Papalas
Attorney/Agent for Applicant(s)
Reg. No. 40,381
Date: April 6, 2006
Telephone No. (214) 855-8186

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 10/037,267

1. A processor-based device that prevents unauthorized use, comprising:
a processor for executing software instructions;
software instructions defining at least one user application;
a wireless communication subsystem that is operable to transmit and receive data utilizing a wireless protocol;
software instructions defining a security protocol process that is operable to prevent execution of said software instructions defining said at least one user application by said processor when a message is received via said wireless communication subsystem, wherein said message indicates that said processor-based device is not in possession of a rightful user;
and
a basic input/output system (BIOS) that is operable to boot said processor-based device and is further operable to verify integrity of said security protocol process before completing boot operations.
2. The processor-based device of claim 1 further comprising:
non-volatile memory, wherein said security protocol process is operable to store information in said non-volatile memory to indicate that execution of said software instructions defining at least one user application is not permitted.
3. The processor-based device of claim 2 wherein said non-volatile memory is flash memory.
4. The processor-based device of claim 1 further comprising:
user data, wherein said security protocol process is operable to prevent access to said user data when said message is received.
5. The processor-based device of claim 1 wherein said security protocol process is operable to cause said at least one user application to exit if said at least one user application is executing when said message is received.

6. The processor-based device of claim 1 further comprising:
a display, wherein said security protocol process causes said display to present information indicating that said rightful user is not in possession of said processor-based device.

7. The processor-based device of claim 1 wherein said security protocol process is implemented in an operating system of the processor-based device.

8. (Canceled)

9. A method for protecting a processor-based device from unauthorized use, wherein said processor-based device performs wireless communication, said method comprising:

receiving notice that said processor-based device is not in possession of a rightful user;

sending a message to said processor-based device to initiate a security protocol via a wireless communication protocol;

receiving said message by said processor-based device; and

initiating said security protocol on said processor-based device in response to said received message, wherein said initiating comprises preventing execution by said processor-based device of at least one user application that is defined by software instructions stored on said processor-based device in response to receiving said message by said processor-based device; and

writing information in non-volatile memory of said processor-based device that said processor-based device is not in possession of said rightful user in response to said received message.

10. (Canceled)

11. The method of claim 10 wherein said non-volatile memory is flash memory.

12. The method of claim 9 further comprising:
preventing access to user data stored on said processor-based device in response to said received message.

13. The method of claim 9 further comprising:
displaying a message on a display of said processor-based device to indicate that said processor-based device is not in possession of said rightful user.

14. The method of claim 9 further comprising:
causing at least one user application to exit if said at least one user application is executing when said message is received by said processor-based device.

15. The method of claim 9 further comprising:
verifying integrity of executable code that implements said security protocol.

16. A system that prevents unauthorized use, comprising:
means for processing software instructions;
means for defining at least one user application;
means for transmitting and receiving data utilizing a wireless communication protocol; and
means for preventing execution of said software instructions defining said at least one user application by said means for processing when a message is received via said means for transmitting and receiving, wherein said message indicates that said system is not in possession of a rightful user, wherein said means for preventing execution is implemented by an operating system of said system.

17. The system of claim 16 further comprising:
means for preventing access to user data that is operable when said message is received.

18. The system of claim 16 further comprising:
means for storing information in non-volatile memory to indicate that said system is not in possession of said rightful user.

19. The system of claim 16 further comprising:
means for displaying information to indicate that said rightful user is not in possession
of said system.

APPENDIX B

Evidence--None.

Application No.: 10/037,267

Docket No.: 10011529-1

APPENDIX C

Related Proceedings--None.